

## ARIZONA ELECTRONIC RECORDKEEPING SYSTEMS (ERS) GUIDELINES

---

Version 2.0 : 2 January 2003

Available online at [http://rpm.lib.az.us/alert/ERSGuidelines\\_v2.pdf](http://rpm.lib.az.us/alert/ERSGuidelines_v2.pdf)

The rise of e-government means a shift from paper to electronic records. As a result, many assumptions about how government uses records need to be rethought. The fundamental need for records has not changed. However, the way records are created, used, and managed in an electronic environment is very different. These guidelines help managers understand those differences, and it helps system designers understand how to address those differences in an electronic environment.

These guidelines describe the basic functions that records serve in the business process. If an electronic recordkeeping systems (ERS) does not include those functions, the records it contains may not be not meet an agency's need for the records, may not be accepted as credible evidence, or may be lost. The guidelines help prevent increased costs from over-engineering in the design phase, expensive management during the system life, and increased risk exposure.

With e-records, the process of creating and managing records is much more important than the format, media, software, or hardware used to create or store the records.<sup>1</sup> Two key principles are fundamental to developing a quality ERS.

- › Records are more than information (content). Records have format (structure) and position within associated records and processes (context) that help ensure that the records are authentic and reliable. In paper-based systems, those characteristics and processes are often so familiar that they are invisible and overlooked when developing system specifications. Unless the complete functionality of records – content, structure, and context – is addressed, the recordkeeping system will be inadequate.
- › Systems and records both have life cycles, but those life cycles are seldom in sync. Designers are often so focused on the creation of a system that they may forget to ensure that records can survive the decommissioning of a system. Emphasis on the business transaction can result in a myopia that focuses on the period of the records' active use and fail to address the entire lifecycle of records. Incorporating records management functions during the development of an ERS makes it significantly easier and less expensive to properly manage the records in the system because the system designers are familiar with the record structure, storage facilities, and processes. Adding records management functions to the software at a later date may be particularly difficult and expensive – and occasionally impossible – because adequate documentation is often missing.<sup>1</sup>

To achieve those goals, it is essential to incorporate the whole of the business process into an automated system. Many automation projects have focused only on the transactions that create records and failed to include those processes that manage the records of those transactions. One of the principal lessons of the past is that retrofitting recordkeeping processes onto existing systems is costly.

These guidelines are intended to minimize the costs of ERS. A key tenet is that costs to implement functionality should be appropriate to the value of and risks associated with the records.

- › Current savings realized during the design of new systems. Development costs can be minimized by ensure that the system is sufficient without being over designed. Implementing recordkeeping functionality after the fact is significantly more expensive.

---

<sup>1</sup> "For conversions to be successful, those performing the transition must have knowledge of the original application and data formats, and the more complex the file structure, the more important this knowledge is. Whether the application is commercial or generated in house, over time this knowledge may be lost and with it the ability to perform a successful migration." United States General Accounting Office, *Information Management: Challenges in Managing and Preserving Electronic Records* (Washington, DC: the Office, 2002), p. 47).

› Future savings can be realized by planning for the inevitable process of migrating to a new system when the current system is obsolete. These savings can be significant.

› Potential cost savings result from minimized risks associated with litigation and open records requests. Failure to address recordkeeping functionality can result in loss of records, resulting in lost intellectual assets and increased risk.

These guidelines will be most useful when designing new systems. However, the guidelines can be used as a standard to evaluate existing systems to determine whether the records in those systems warrant the expense of at least a partial retrofit.

These guidelines do not apply to all e-records. They are most useful for relatively closed systems which manage routine business processes and the records they produce. The guidelines do not apply to open systems containing non-routine, heterogeneous e-records.

## Overview

These specifications are organized into four broad sections.

- I. Assessing the value and risks associated with records. Because different records have different value and risks, the level of compliance with these guidelines will also differ. The section for managers and system designers explains how to scale these guidelines – and the resources necessary to implement them – to a particular recordkeeping system.
- II. Responsibilities for recordkeeping are divided among a number of players, especially in the electronic recordkeeping environment. The agency has primary responsibility for its own records, but other agencies establish guidelines and implement laws that impact how the agency manages its records. This section describes the different agencies that impact electronic recordkeeping.
- III. General recordkeeping requirements in a governmental context to help designers to fully understand the business value of records by explaining how they are used (especially after the transaction that produced them is finished). This section introduces key characteristics of e-records, including trustworthiness, records management, legal requirements, business requirements, security requirements, administrative considerations, and human factors.
- IV. Specific functional requirements for a recordkeeping that – along with business requirements – should be incorporated into any automated system that creates records. This section provides managers and system designers background on these requirements, and gives system designers details on how to implement the requirements. The functional requirements relate to system administration, the origin/creation of records, security and trustworthiness, access, maintenance and preservation, and disposal.

Three appendices provide additional information

- A. Acknowledgement of the sources used in this document and the individuals who worked on it.
- B. Archival appraisal standards, which help users understand which records are likely to require permanent preservation.
- C. These Guidelines are based on the National Electronic Commerce Coordinating Committee's (NECCC) "Electronic Records Management Guidelines for State Governments" and on the Delaware Public Archives' "Model Guidelines for Electronic Recordkeeping Systems." Cross references to these documents are represented in the text by Roman numerals in superscript. The text of the notes are in this appendix.

## I. ASSESSING THE VALUE OF RECORDS<sup>ii</sup>

Addressing the challenges of e-records requires appropriate resources, and an ideal system may be quite expensive. The effort and expense necessary to design an ERS should balance the value of the records against the potential benefits and costs of automation. Just as with paper records, the e-records an agency produces or receives are not all of equal importance or value. For example, it may make little sense to invest large sums of money in a system that contains records that are of transitory value and pose little risk of litigation. While an ideal ERS would offer many possible recordkeeping features, in practice an ERS should not attempt to implement a higher standard of recordkeeping practices than is appropriate to a trustworthy manual (paper-based) recordkeeping system unless there is a clearly demonstrated benefit or business need.

The following factors should be considered in assessing the value of the records.

### *Business and Administrative Value*

Records' primary value results from their ability to help the agency support its ongoing, day-to-day administrative affairs, document legal obligations and to protect legal rights, and to establish fiscal responsibility and accountability. The primary value of records almost always diminishes over time. Records that are no longer of value to the agency and are no longer in active use, should be disposed of by destruction or by transfer to the State Archives.

### *Level of Risk Exposure*

Risk management requires an analysis of potential for harm to the agency or to others, relative to potential benefits. Risk management also must consider alternative measures to address risks and the implementation of measures that best address risk based on this analysis. In applying risk management to e-records, the following questions should be asked.

- › What would be the impact on agency operations if the records were lost or otherwise unavailable?
- › Would the agency or others suffer a financial loss if the records were unavailable?
- › What is the likelihood that the records would be subject to or needed for a legal action?
- › Would the inability to produce the records in a form admissible in court have a critical impact on the outcome of a case?

For more information on risk management, see

- › Arizona Government Information Technology Agency (GITA). *Risk Management Standard*, P800-S805. ([http://gita.state.az.us/policies\\_standards/pdf/p800-s805%20risk%20management.pdf](http://gita.state.az.us/policies_standards/pdf/p800-s805%20risk%20management.pdf))
- › NIST *Risk Management Guide for Information Technology Systems* 800-30 (January 2002, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>).

### *Archival Value*

A small percentage of records have enduring value that warrants the expense of long-term preservation. More often than not, archival records are valuable for their secondary value – information useful to someone other than the agency which created them.

The Arizona State Archives identifies, collects, preserves, and provides access to records in all formats of Arizona state and local governments and of public officials and other individuals. Archival records remain useful for the Legislature, state agencies, and the general public because those records enable citizens to hold government accountable; provide evidence about public policies and programs;

and protect or verify individuals' rights and entitlements. Archival records provide information about the important people, issues, places, and events that make up the story of Arizona's history.

The State Archives has published a more complete description of the appraisal criteria it uses to determine if records are permanently valuable. For more information on archival value, see *Appraisal Criteria for Archival Records* (Appendix A).

### *Benefits of an ERS<sup>ii</sup>*

Records are the corporate memory that capture an agency's information assets. Often they have been painstakingly assembled at great cost. Good recordkeeping is the basis of knowledge management, allowing an agency to make the most of its intellectual capital and operate more efficiently by ensuring that

- › Users can find information quickly, increasing the quality of customer service.
- › Management decisions are based on complete and accurate information.
- › Resources are not wasted, saving time and money spent collecting the same information multiple times.
- › The costs of storing and preserving records is minimized by destruction of obsolete records.
- › The costs of migrating to a new software or hardware platform are minimized by incorporating the migration process into system design.
- › The costs of producing all relevant records during discovery is minimized. Discovery orders require that all relevant documents be produced. Developing a classification scheme to indicate where potentially relevant records are stored and disposing of obsolete records (especially copies on backup tapes) to reduce the volume of records that must be searched can save significant time and money during searches. Potentially more important, good recordkeeping ensures that all relevant documents are produced; late discovery of additional relevant records can damage the agency's credibility with the court.

The use of technology to automate recordkeeping can offer significant savings in staff resources; fewer people are required for filing and retrieving information. Work can be much more efficient; less time is necessary to access information and many people can work in the files simultaneously. E-records require significantly less office space for storage. Quick, inexpensive duplication of e-records makes off-site records storage practical, offering significant protection against disaster. At the same time, hardware, software, support personnel, maintenance costs, and system migration can quickly counter cost savings.

Finally, the tragedy of the September 11 attacks demonstrated an important benefit of e-records over paper records. Because e-records can be duplicated easily and at relatively little cost, it is practical to keep a copy of all records at a secure site for disaster recovery and business continuity. Many companies were able to open for business the next day because they could work from copies of their records stored offsite. The State Library and Archives strongly supports the well-managed use of e-records as one of the most effective measures an agency can take to ensure business continuity and disaster recovery.<sup>2</sup>

### *Practical Limits of an ERS*

All government records should be well managed to ensure that they are preserved, accessible, and disposed of properly. However, the effort and resources a state agency expends to manage records, including e-records, should be related to the level of risk associated with the information contained in the

---

<sup>2</sup> ARS §41-1345 requires that agencies implement an essential records program.

199 records. Recordkeeping systems containing high-risk records will need greater controls (with a greater  
200 expense) to ensure reliability and trustworthiness than would a system containing low exposure records.  
201  
202 In the long run, the decision to implement an ERS must balance risks, benefits, and costs relative to the  
203 value of the records. Just because it's possible to do something electronically doesn't mean it makes  
204 good sense. Traditional recordkeeping techniques can be married to an ERS to find the right balance.  
205  
206

## II. RESPONSIBILITIES FOR RECORDKEEPING

Recordkeeping is one of the most basic functions of government agencies. People rely on government to maintain social order by tracking important public information, ranging from birth and death certificates to property records. Records track the government's activities, ranging from tax collection to development of major programs through legislation.

In a democracy, access to records enables the public to hold government officials and employees accountable. The information contained in government records documents past and current actions, decisions, procedures, and policies, and may reveal unacceptable inefficiencies or a failure to follow procedure. The failure to create or the destruction of records opens government to accusations of fraud, impropriety, or political embarrassment.<sup>3</sup>

An underlying principle of democratic government is that public records are the people's records, and the officials who hold the records are merely trustees for the people. As trustee of the people's records, government is responsible for

- › maintaining, protecting, and preserving the information entrusted to it;
- › assuring prompt access to the information,
- › securing the confidentiality of the information that is not subject to disclosure,
- › ensuring the content, context, and structure of the original information is not compromised,
- › ensuring that individuals associated with origination, modification, or authorization of information are identified and can be verified over appropriate time.

An agency's automation of its business processes should continue to uphold the people's trust by establishing policies and procedures to address the access, security and retention requirements associated with information derived and transmitted from its records. An agency must establish controls and practices to ensure that its information is accessible and secure. The integrity, availability, recoverability, and appropriate use of all information assets must be ensured throughout the processing of that information.

### *The Role of State Agencies*

Every agency must create sufficient records to document its work based on a number of factors, balancing the value of the information, the risks associated with disposal of the information, and resources necessary to capture and maintain the records over time. Once an agency has established the records necessary to be created, Arizona statute requires the agency to establish and maintain an active, continuing program for the economical and efficient management of its public records (ARS §41-1346).

Each agency must designate an individual to manage its records. In particular, staff members should be assigned responsibility for managing the ERS and provide evidence of their assignments through position descriptions, administrative memoranda, or other transmitted means.<sup>iv</sup>

### *The Arizona State Library and Archives' Regulatory Role*

The State Library and Archives is mandated to oversee the management of public records throughout state and local government in Arizona (ARS §41-1345). The Library and Archives accomplishes its mandate through its Records Management Division by issuing regulations, policies, and procedures, and by publishing guidelines and standards that establish acceptable practice for government agencies.

---

<sup>3</sup> See Kansas Electronic Records Management Guidelines, <http://www.kshs.org/archives/ermguide.htm#2>.

The Records Management Division offers workshops and consults with government agencies to ensure that the agencies have an effective and efficient records management program in place and operates a center for storing inactive records pending disposal. One of the Division's most important functions is to work with agencies to develop records retention schedules indicating how long record series must be kept.

Under the auspices of the Arizona Historical Records Advisory Board (AHRAB), the Library and Archives established the Arizona 'Lectronic Records Taskforce (ALERT) to coordinate e-records activities in state and local government and to identify best practices for managing those records.

The State Library and Archives also is mandated to preserve records of permanent value created by state agencies. The ability to preserve e-records requires collaboration between agencies and the State Archives to ensure that the information is transferred in a stable format and organized in a manner that will support access.

#### *Other Agencies' Roles*

A number of state agencies have an oversight and regulatory role in e-government and the management of e-records.

Department of Administration, State Procurement Office. Concerned that purchase of recordkeeping systems is cost effective.

Auditor General. Relies on records to ensure that the agencies are fulfilling their mandate effectively, using resources wisely, and complying with the law. The Auditor General may also review agencies' recordkeeping programs to ensure that there is sufficient information for financial and program audits.

Government Information Technology Agency (GITA). Provides oversight and coordination for the state's Executive Branch automation resources and advises the three braches of state government about information technology. GITA has developed research alliances with the public and private sectors to review and evaluate emerging technologies for use in state government. GITA also evaluates agency information technology projects with development costs exceeding \$25,000.

Secretary of State's Office. Oversees compliance with electronic signatures regulations.

Because these agencies have overlapping interests in electronic recordkeeping systems, they are important partners in the Arizona 'Lectronic Records Taskforce (ALERT).

### III. GENERAL REQUIREMENTS FOR RECORDKEEPING

#### General Requirements for Trustworthiness

Although computers have changed the form of records, their fundamental purpose remains the same. Agencies continue to keep records in order to provide services, to present evidence, to provide historical documentation, to preserve its heritage, and to allow its actions to be reviewed and audited.

#### *Content, Context, and Structure*

The fundamental nature of a record as a authentic, reliable memory remains the same. In order to build an effective, efficient ERS, it is necessary to be familiar with the essential characteristics of a record and the recordkeeping process. Unless those characteristics are reproduced in the electronic environment, e-records may not be trustworthy.

In order to ensure that e-records are trustworthy, an ERS must not only include the same information (content) in a paper recordkeeping system, but must also capture information about the records' context and structure to be able to test for authenticity, reliability, and integrity. The latter, which are often inherent in the physical characteristics of individual paper records or the manner in which they are managed, is typically captured as metadata for e-records.

- › Content is the substance of a record – the text, data, symbols, numerals, images, and sound – that captures sufficient information to provide evidence of a business transaction.<sup>4</sup>
- › Context refers to the business and technical environment in which a record is created. Contextual information is often extrinsic to the record itself. In a paper record, this information may be captured through physical location (custody) or through policies or procedures that dictate how the record is handled. Because several records may be necessary to complete a single transaction, especially in an electronic environment, context is particular important to ensure that all records relevant to a transaction are appropriately linked.
- › Structure includes physical characteristics of the record, as well as the internal organization of the formal elements of the record's content and the record's associations and relationships to other documents. Structure may associate an individual record with other records in the same series, in the same dossier, or to other members of a compound document. Structure may include information about fonts; line, paragraph, and page breaks, and or about other editorial devices that affect the understanding of the document. For example, the space visually defines the elements of a table and gives meaning to the contents of those elements in terms of columns and rows.

The context and structure are important means to test the authenticity, reliability, and integrity of a record. For paper records, handwriting may be used to authenticate the author, inks and papers may be used to verify dates. For e-records, a significant portion of the context and structure of the record may be embedded in software and hardware, external to the record and easily dissociated from the record.<sup>5</sup>

<sup>4</sup> "[Content] encompasses the complete set of documentation required to provide evidence of a business transaction," Center for Technology in Government, State University of New York at Albany. *Practical Tools for Electronic Records Management and Preservation* (Albany: the Center, 1999).

<sup>5</sup> The separation of content from contextual and structural information in automated systems is reflected in the 1997 Federal District court decision in *Public Citizen v. John Carlin* (2 F. Suppl. 2d 1 (D.D.C. 1997)) which notes that an electronic message is not necessarily equivalent to its printout. "[The] difference between electronic and paper records illustrate the fact that the administrative, legal, research, and historical value of electronic records is not always fully captured – indeed, is usually not captured – by paper or microfiche copies. Electronic records therefore do not become valueless duplicates or lose their character as 'program records' once they have been printed on paper; rather, they retain features unique to their medium."

With e-records, the process of creating and managing records is much more important than the format, media, software, or hardware used to create or store the records.<sup>v</sup> Because e-records may be moved within or between systems, tests for authenticity of e-records seldom rely on the physical carrier; rather, tests for authenticity look at the use, accessibility, and custody of the records. An ERS must include the functionality to not only capture the content of the business process in the record, but also that its context and structure are captured (typically in metadata documenting the process) to demonstrate the records' authenticity and reliability.

Unless an electronic system respects the particular requirements of recordkeeping, the information it contains may not be accepted as evidence on the grounds that it is not reliable, is not authentic, or has been altered. Without authentic, reliable, and legally acceptable e-records, e-government may falter or fail. Incorporating sound records management principles in an ERS will ensure that the public, corporations, and others doing e-business with the government can have confidence that the ERS is trustworthy.

#### *General Requirements for Authenticity, Reliability, and Integrity<sup>vi</sup>*

One of the most important features of records is that they are trustworthy. Records are expected to be consistent over time, that they have not changed or become corrupt, and that the information they contain and preserve is acceptable as evidence. An ERS can be made untrustworthy if data entry is sloppy, or if unauthorized users gain access.

Trustworthiness is assessed in terms of a record's authenticity, integrity, and reliability. These terms are slippery because they are interrelated and because they are often used interchangeably.<sup>6</sup> Underlying all three concepts is the notion of genuineness, legitimacy, and correctness (veracity). This document will use the following definitions for authenticity, reliability, integrity, and trustworthiness.

- › Authenticity: the quality of being an original (or a true and faithful copy) that can be proven to be what it purports to be; that internal claims (e.g., date, author, content) can be verified; genuine, not false, counterfeit, or altered.<sup>7</sup>
- › Integrity: the quality of being complete and unaltered through tampering or corruption.<sup>8</sup>
- › Reliability: the quality of being a full, accurate representation of the transactions, events, or facts as understood at the time.<sup>9</sup>

<sup>6</sup> "Practitioners' understanding and usage of the concept of 'authenticity' and associated concepts are closely related to their working practice and the context of their work experience. Records users and practitioners deal with records every day in their work processes, where they judge the authenticity of records as needed. Through those processes, practitioners have come to create and understand a working concept of authenticity in their own minds. . . . The language used by practitioners to express issues of authenticity differs significantly from the language used by the most prominent research projects." Eun G. Park, "Understanding 'Authenticity' in Records and Information Management: Analyzing Practitioner Constructs," *American Archivist* 64:2 (Fall/Winter 2001), p. 288.

<sup>7</sup> "Validating authenticity entails verifying claims that are associated with an object – in effect, verifying that an object is indeed what it claims to be, or what it is claimed to be (by external metadata)." . . . "It is important to note that tests of authenticity deal only with specific claims (for example, 'did X author this document?') and not with open-ended inquiry ('Who wrote it?'). Validating the authenticity of an object is more limited than is an open-ended inquiry into its nature and provenance." From Clifford Lynch, "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust," *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, 2000), p. 5-6. Available at <http://www.clir.org/pubs/reports/pub92/contents.html>.

<sup>8</sup> Note: Corrections to a record made according to established procedure and with proper authority do not affect reliability.

<sup>9</sup> "A reliable record is one that is capable of standing for the facts to which it attests. Reliability thus refers to the truth-value of the record as a statement of facts and it is assessed in relation to the proximity of the observer

› Trustworthiness: the capability of producing authentic, reliable records of unquestioned integrity. In order to ensure the trustworthiness of records, an ERS must address a variety of factors relating to the recordkeeping process, rather than characteristics inherent in the record itself.<sup>vii</sup>

Because it will be necessary to have hybrid paper, e-record systems for the foreseeable future, an agency must establish business rules for establishing the authentic copy of a record if there is a discrepancy between the paper and electronic versions. Those processes must be based on established policies and procedures that will stand up to an audit.<sup>viii</sup>

Deviations from established policies and procedures raise flags about the authenticity and reliability of the records. Records with irregularities may be challenged as not credible. Hence, it should be difficult – if not impossible – to circumvent those policies and procedures. The ERS should be part of a larger records management program that includes audits to verify that policies and procedures are followed and that include problem reporting and resolution procedures.<sup>ix</sup>

For best practices on system trustworthiness, see Minnesota's Trustworthy Information Systems Handbook (<http://www.mnhs.org/preserve/records/tis/tableofcontents.html>).

For information on data quality to support reliability, see the United States Office of Management and Budget, "Guidelines for Ensuring and Maximizing the Quality, Objectivity, and Integrity of Information Disseminated by Federal Agencies" ([http://www.whitehouse.gov/omb/inforeg/iqq\\_draft\\_guidelines.pdf](http://www.whitehouse.gov/omb/inforeg/iqq_draft_guidelines.pdf)).

## **General Requirements for Recordkeeping and Records Management**

All Arizona agencies are required by law to have a records management program in place to accomplish these goals.<sup>10</sup> Records management systematically links business processes to records – in paper or electronic format – in order to

- › Capture or create (record) the information necessary to support and document the process.
- › Ensure that the records are accessible (can be located) as long as they are needed.
- › Retain records as long as they are needed to support the entire process (including reference after the transaction which generated the record is completed). Those retention periods are defined on a records retention schedule developed specifically for the agency or on a general schedule issued by the Library and Archives Records Management Division.
- › Ensure that the records are protected from unauthorized alteration or loss.
- › Dispose of records properly, either by destruction or transfer to an archives.
- › Balance the costs of records programs (including the costs of programming sophisticated recordkeeping functionality into an ERS) against the value of and risks associated with the records.

Systems designers and records managers should work together to design an ERS to properly manage the records it contains. Key factors to consider when developing an ERS include

---

and recorder to the facts recorded." From Heather MacNeil, "Trusting Records in a Postmodern World," *Archivaria* 51 (Spring 2001), p. 39.

<sup>10</sup> Records management includes the creation and implementation of systematic controls for records and information activities from the point where they are created or received through final disposition or archival retention, including distribution, use, storage, retrieval, protection and preservation (ARS §41-1346D).

- › Manual recordkeeping systems are often imperfect. When automating an existing system, all business processes that cause records to be created, retrieved, preserved, or disposed should be carefully examined and re-engineered when necessary.
- › Special care must be taken to ensure that people have the same trust in e-records that they have in paper records. For example, it is essential that e-records be accepted as evidence in courts. The familiarity of paper records, as well as assumptions, practices, and laws relating to records that give people confidence in paper records do not readily translate into the digital environment.
- › The nature of automated record systems introduces new problems that must be addressed. Because people are familiar with paper records, they often have an unconscious ability to verify records. Even individuals with an untrained eye may spot odd paper or ink; irregular or missing signatures or dates; or erasures and may question a record that ‘doesn’t look quite right.’ Because e-records are easier to change, and because those changes do not leave readily apparent clues, an ERS should include the ability to detect unauthorized changes.

For research on e-records requirements for reliable evidence, see Wendy Duff, “Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC,” *Archivaria* 42 (Fall 1996).

### **General Legal Requirements<sup>x</sup>**

Arizona law requires all agencies to “Make and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency designed to furnish information to protect the rights of the state and of persons directly affected by the agency’s activities” (ARS §41-1346).<sup>11</sup> Federal or state laws may require specific agencies to keep certain records or to keep records in certain formats. When designing an ERS, the agency should consult with legal counsel to determine legal requirements for recordkeeping.

Laws and regulations often dictate retention periods for specific types of records or place requirements on the content or nature of those records. Consult with the Library and Archives Records Management Division, which has extensive knowledge of legal requirements for retention periods.

Agencies are required by law to make virtually all records available to the public (ARS §39-121). At the same time, some information in records must be redacted to protect confidentiality or privacy. During the design process, an agency should establish policies and procedures for providing the public with the records and ancillary information contained in an ERS while filtering any information that should be restricted on grounds of privacy, confidentiality, or security classification.

Agencies must be able to produce all records relevant to litigation. Records that are relevant to pending or current litigation must be preserved, even if their retention period has passed. Discovery of all relevant records can be complicated by the presence of copies of relevant records in many places. In addition to searching the active recordkeeping system, agencies must also search backup media.

To minimize the costs of discovery, it is essential that an agency be able to demonstrate with confidence a routine process that protects data until it is obsolete and then deletes all copies from the system (including backups).

### **General Business Requirements<sup>xi</sup>**

Agencies create and preserve transactional and informational records<sup>12</sup> in order to fulfill their mandate. Arizona law requires “all officers and public bodies to maintain records . . . reasonably necessary to

<sup>11</sup> Arizona law mandates that all officers make and maintain records reasonably necessary to provide knowledge of all activities they undertake in furtherance of their duties. See 21 Ariz. D 2d, p. 153. *Carlson v. Pima County*, 687 P.2d 1242, 141 Ariz. 487.

<sup>12</sup> The legal definition of a public record in Arizona is particularly broad, including virtually all information that is created or received in an agency that is useful enough to be kept for a period of time. In some instances, that

provide an accurate accounting of their official activities and of any government-funded activities” (ARS §39-121.01(B)).

When designing an ERS, the agency must clearly define the records created by the business process being automated by establishing

- › When information should be transformed from draft information to a formal record. Creating a static snapshot of information at a moment in time that encapsulates the content, context, and structure of the record is especially important for documents that are created using databases, spreadsheets, or other tools that are not designed to preserve previous versions and are likely to be overwritten.
- › The content necessary for a sufficient record. Typically, the content may include a date, and the names and signatures of parties and witnesses, in addition to the substance of the record.
- › The necessary structure of the record, including acceptable variation in presentation formats due to changes in technology.
- › Contextual information about the execution of the record, often captured in metadata, documenting the process used to generate a transaction or that reference other records necessary to understand the current record.
- › Sufficient audit trails to demonstrate legal, financial, contractual, or program accountability.
- › That any financial functions conform to generally accepted accounting principles and to applicable legal and contractual provisions.

## **General Security Requirements**

Traditional paper records were protected from unauthorized access through physical controls. For example, placing files where people could see who used them, locks, and – for very sensitive data – access logs. Changes to the documents could be detected by physical clues, such as erasures, forgeries, and inks.

Because of the ability to access systems remotely and the fragile nature of electronic data, system designers must implement mechanisms to restrict access and to ensure the integrity of the record. System specifications should establish the level of security, which is related to the level of risk, to ensure that the system is neither over or under engineered.

For more information on general security requirements, see GITA’s policies and standards.<sup>13</sup>

## **Other Administrative Considerations**

An ERS must work within the current economic and governmental environment to balance a variety of legal, business, and technical requirements. When designing an ERS, the agency must work carefully with the system designer to achieve a fundamental goal of records management: to ensure that the costs of incorporating these requirements into the system are justified by the value of the records.

In order to help systems designers balance costs and benefits, the Library and Archives has posed certain assumptions about the current state of ERS in Arizona. The following assumptions reflect the current environment and are subject to revision as that environment changes.

---

information is in the form of a transactional record that documents a routine business procedure. In many cases, records are neither routine nor transactional; examples include notes, working papers, and correspondence, which may be in word processing files, spreadsheets, or email messages. See American Jurisprudence, 2nd. Records §26.

<sup>13</sup> [http://gita.state.az.us/policies\\_standards/](http://gita.state.az.us/policies_standards/)

- 496 › Manual and electronic recordkeeping systems will exist side by side for the foreseeable future.
- 497 Manual systems may need to be modified and ERS must be designed so that the two systems are
- 498 well coordinated.
- 499
- 500 › ERS are relatively new. A lack of consensus on best practices places any information kept in an
- 501 ERS at some risk of loss. That risk can be mitigated with good planning and – given the benefits of
- 502 the ERS – may be entirely acceptable for many records. In general, risk increases with the length of
- 503 time records must be retained. Agencies should proceed with caution when dealing with records that
- 504 must be kept for more than ten years and, depending on the level of risk, consider backing up the
- 505 records in a stable format such as computer output microfilm.
- 506
- 507 › Few agencies will have additional money for targeted e-records efforts. They will have to pull a
- 508 percentage of resources from existing activities; some activities may be discontinued, while others
- 509 may be scaled back.
- 510
- 511 › The State Library and Archives has redirected funds to help agencies develop policies and
- 512 procedures to develop strong e-records management programs.
- 513
- 514 › Agencies will have to bear the costs of managing their e-records – current and inactive – throughout
- 515 the records' lifecycle, which includes the costs to migrate to new ERS software/hardware or to a non-
- 516 electronic format. Agencies are not responsible for costs associated with preserving or providing
- 517 access to their records that have been accepted by the State Archives.
- 518
- 519 › Archival information – the three to five percent of permanently valuable information – may be lost if
- 520 agencies store that information exclusively in e-formats before standards and practices for
- 521 permanent preservation of e-records are well established. Until best practices are established,
- 522 archival information should not be kept exclusively in electronic format. When e-records of archival
- 523 value are no long active, they should be transferred to durable media such as computer output
- 524 microfilm or paper, typically in an annual batch.
- 525
- 526 › People are at the heart of any recordkeeping system, paper or electronic. Because records
- 527 management requires people to follow policies and procedures, the quality of recordkeeping is
- 528 human and imperfect. The quality of records management will vary from agency to agency. When
- 529 agencies have a strong business need for good records, they will invest necessary resources to
- 530 ensure good records management.<sup>14</sup>
- 531

## 532 Human Factors

533 Finally, recordkeeping has always been dependent on human behavior, and that behavior is often  
 534 imperfect. The mechanical nature of computing allows an ERS to be designed in such a way that it  
 535 compensates for some of those imperfections. An ERS can greatly increase records' reliability by  
 536 including automated error checking to validate data and ensure that records are complete.

537 Systems designers must remember that users – both those who enter data, as well as those who  
 538 retrieve it – are ultimately the heart of the system. If the system is difficult to use or difficult to understand,  
 539 users may circumvent the process, making the ERS less reliable because information is missing or  
 540 inaccurate. Such work-arounds often are not an attempt at fraud, but an attempt to enter information  
 541 through a 'back door' to get the correct result if they cannot enter it through the 'front door.' Or, users

---

<sup>14</sup> Although not a direct study of Arizona's recordkeeping practices, the National Archives and Records Administration's *Report of Current Recordkeeping Practices within the Federal Government* likely translates closely to Arizona's recordkeeping environment. The authors note, "The quality and success of recordkeeping varies considerably across the agencies studied . . . . When agencies have a strong 'business' need for good [recordkeeping], such as the threat of litigation or an agency mission that revolves around maintaining 'case' files, then [recordkeeping] practices tend to be relatively strong *with regard to the records involved*." [Emphasis in original.] (p. 5) [http://www.archives.gov/records\\_management/pdf/report\\_on\\_recordkeeping\\_practices.pdf](http://www.archives.gov/records_management/pdf/report_on_recordkeeping_practices.pdf).

may track information on paper outside the system; although they may intend to enter the information later, date and time stamps will be inaccurate and often the information is never entered.

Training is a significant component to compensate for human factors. Training should include information about the general recordkeeping requirements described above, as well as the use of a specific ERS.<sup>xii</sup>

For more information on human factors, see Jakob Nielsen's *Human Factors Engineering* and his Web site at <http://www.useit.com/>.

It is essential to remember that the diversity of users makes it very difficult to make assumptions about their skills or knowledge. Users are, by definition, average; a system may target the middle ground, but should also establish baseline expectations for designers. If individuals are likely to use the system frequently, designers may want to include some features to simplify use by power users.

#### 557 IV. FUNCTIONAL REQUIREMENTS FOR RECORDKEEPING SYSTEMS

558 An ERS must be able to receive, capture, or create records. It must be able to provide selective access to  
559 the records and ancillary information in the system based on a user's rights to data. It must be able to  
560 maintain and preserve those records over time. Finally, it must be able to dispose of records, either by  
561 deleting records from the system or by transferring them to a durable medium for permanent retention by  
562 the State Archives.

563  
564 The following sections detail specific ERS requirements in terms of records origin, access, preservation,  
565 and disposal. The requirements are stated in terms of general principles, with pointers to guidelines for  
566 best practices and supporting technical standards.

#### 567 Requirements for System Administration

- 568 › **An agency must accurately document the ERS system performance and keep such**  
569 **documentation current.**<sup>xiii</sup> Such documentation should  
570 › Assign system management roles and responsibilities.  
571 › Define the roles and responsibilities of the individuals involved in the creation, maintenance, and  
572 destruction of the records. This may also require roles of individual users.  
573 › Provide for consistent quality control, problem resolution, and other activities that might be  
574 subject to inconsistent action or misinterpretation.<sup>xiv</sup>  
575  
576 › **An agency should routinely test an ERS to ensure the reliability of the software and**  
577 **hardware.**<sup>xv</sup> The audit should address the quality of data when entered, security of access, etc.<sup>xvi</sup>  
578  
579 › **An agency should ensure that users are well trained.**<sup>xvii</sup> Because an ERS is ultimately human-  
580 based, it is essential that the individuals who use and manage the system receive adequate training  
581 in all aspects of the system.

#### 582 Requirements for Origin/Creation

583 An ERS must be able to capture the information necessary to adequately document business processes,  
584 the content of the record. It must also include sufficient information about the context and structure of the  
585 record in order to ensure that the records are acceptable as evidence.

586  
587 Specific requirements include the following.

- 588  
589 › **Documented procedures for the receipt, creation, processing, and filing of e-records.**<sup>xviii</sup>  
590 These policies and procedures should indicate required administrative, contextual, structural, and  
591 preservation metadata; acceptable formats; the conditions that must be met to ensure that the  
592 creation or transmission is complete and that the record has been stored in an immutable form.  
593 Policies and procedures should include routine checks on quality control and mechanism for  
594 addressing quality problems. Data entry routines should validate data.  
595  
596 › **Create or capture a record for each business transaction.**<sup>xix</sup> The record must include sufficient  
597 content, context, and structure to meet business and legal needs as dictated by the nature of the  
598 transaction. A record should have at least four elements to be considered complete: date, the  
599 identification of creator(s), the addressee(s), and the action. However, records often need additional  
600 elements to be truly useful.  
601 The following common elements are listed for reference and are not mandatory.<sup>15</sup> If the  
602 following elements are not explicitly part of the content, they may be captured as metadata supplied

<sup>15</sup> See InterPARES UBC Project, "Rules for Activities Involved in Managing Archival Framework." Available online at <http://www.interpares.org/UBCProject/tem6.htm>.

by the system. Many of these elements may be system supplied, either as a default for the series as a whole or as a specific value for an individual record.

#### *Content Elements*

These elements typically appear within the body of the record. However, some elements may exist only as metadata, or redundant metadata may be created to facilitate indexing and access of the record's content.

1. *Date*.<sup>xx</sup> Includes both the time and place when the record was compiled or issued. For transactions where the parties may be at different locations, all locations should be noted. Should include the time of transmission (to an internal and/or external addressee) and time of receipt. Also referred to as chronological date and topical date (location).
2. *Identification of Creator(s)*. The name, title, and address of the agency or individuals creating the record. This information typically appears in the letterhead of paper records. Individuals acting as agents for an agency, organization, or corporation should also be identified by name and role. Also referred to as entitling.
3. *Addressee(s)*. The name, title, and address of the individuals to whom the record pertains. The addressee is often omitted from records intended to publish information generally rather than directed to an individual; e.g., certificates. Addressees must be distinguished from recipients. Also referred to as the inscription.
4. *Recipients*. Names of other individuals or organizations who received a copy of the record. Records that must be formally recorded for public notice should use this element to note that action.
5. *Action*. An expression of the decision or will of the record creator. Also called disposition.
6. *Subject*. A brief statement indicating what the record is about. The identification of content, including the date of the event, fact, or act represented, if different from the date of the record. While traditional non-textual records do not always have a title or subject, non-textual records in electronic form, just like the textual ones, always include a one line title (which is usually called "file name") that is often the subject of the record. This is not sufficient for either textual or non-textual records.
7. *Preamble*. The intent or motivation for the act underlying the record, ethical or legal principles on which the record is based. Rare, except in the most formal documents.
8. *Body*. The concrete and immediate circumstances of the act underlying the record. Also called the exposition.
9. *Final clauses*. Includes attestations (identification of those who took part in creation of the record, such as authors, witnesses, etc.) and secretarial notes.

#### *Contextual Elements*

Unlike content, contextual elements are typically extrinsic to the record. Where content captures the information that the record is *about*, contextual information captured information necessary to understand the history of the record. Because context is crucial for ensuring the authenticity and reliability of the record, appropriate implementation of these elements is essential to creating a trustworthy system.

1. *Unique Identifier*. Each record should have a unique code for the record.<sup>xxi</sup>

2. *Transaction identifier.* Each transaction should have a unique code that can be used to link all records relating to that transaction.
3. *Intellectual Classification.* Information assigned by the agency to organize or file records. Classification may be by content, genre, or both. Classification by content typically uses a standard vocabulary or file plan. Classification by genre identifies conventions or documentary types which may indicate content, internal structure, or function; examples include agenda, contract, correspondence, license, press release, proposal, and report.
4. *Access Classification.* Any conditions relating to access of the records, including restrictions due to privacy, confidentiality, or security. Access may be assigned at a record level or, to redact specific information, at the field level.
5. *Digital Signatures.* An electronic signature used to ensure the identities of individuals who have signed the record or a message digest or hash value used to demonstrate that the content of the record has not been changed.
6. *Use History.* Includes dates and descriptions of access and use of a record, from the time of its receipt/capture to its disposition. This element is particularly important for records covered under the Health Information Portability and Accountability Act (HIPAA).
7. *Retention Period.* The length of time a record must be retained. May be implemented as a link to a records retention schedule.
8. *Management History.* Records management actions performed on a record (with date) from its receipt/capture to its disposal; often done in batch based on the series to which the record belongs or recorded as part of another function. Actions include access classification review, audit, close, hold, disposal changed, disposed, released, and retention period changed.
6. *Preservation History.* Dates and actions taken to ensure that the record remains accessible and readable throughout its life. In particular, notes should indicate any known degradation of the record, such as imperfect migration of formatting between reader applications or application versions.

#### *Structural Elements*

Unlike contextual elements, structural elements are intrinsic to the record. Like contextual elements, structural elements are often overlooked because they are not part of the content. Rather, these elements organize and format the content to make it meaningful. In e-records, structural information is often captured in metadata.

1. *File Details.* File size and format. Because an e-record is a bitstream that is independent of a specific storage medium, it is generally not necessary to track storage media (tape, disk, CD-ROM). However, capturing this information at the series level may be useful for long term management of offline records.
2. *Format.* The logical form (content medium and data format) and physical form (storage medium and extent) of the record. Examples of content medium include audio, image, text, video, and compound. Examples of data format include ASCII, comma separated values (CSV), jpeg, Word doc, and Adobe PDF. Examples of storage media include CD-R, DVD, DAT, and DLT. Format may also include information about order and position of the elements, as well as fonts.
3. *Language.* Note the specific machine language (EBCDIC, ISO Latin-1, etc.) or human language (English, Spanish) of the record.
4. *Encryption Details.* Information on how a record has been encrypted.

5. *Relations*. Links to other information or between the component documents that comprised a single record.

› **All records created by the system must belong to a records series listed on the agency's records retention schedule.**<sup>xxii</sup>

› **The recipient should provide the send a receipt confirming delivery of the record.**<sup>xxiii</sup>

For information on additional schemes to capture contextual, structural, preservation, and other metadata, see the following.

› *Data Dictionary - Technical Metadata for Digital Still Images*: NISO Z39.87-2002, AIIM 20-2002. Draft available for review from 1 July 2002 through 31 December 2003 at [http://www.niso.org/standards/resources/Z39\\_87\\_trial\\_use.pdf](http://www.niso.org/standards/resources/Z39_87_trial_use.pdf).

› Minnesota Recordkeeping Metadata Standard (IRM 20), available at <http://www.mnhs.org/preserve/records/metamrms.pdf>

## Requirements for Ensuring Security and Trustworthiness

The process of user authentication is closely tied to system security. In a perfectly secure system, it would be impossible for someone to assume another user's identity to gain access to the system either to view or modify records. Not all records demand the same level of security. Alterations to an online staff phone directory will likely have significantly less risk than changes to the accounting records.

An ERS must protect records against change over time, either through unintended side-effects of software or through unauthorized access to the system. Other security considerations include user behaviors, including unsecured work stations, shared or easy-to-hack passwords, and social engineering hacks.

Specific requirements for general system security and trustworthiness should include the following.

› **Determine appropriate levels of security.** Security is based on risk and legal requirements, and select an appropriate authentication protocol (e.g., shared secret, PIN, or biometrics) and secure method of transmission during data entry or submission (e.g., Public Key Infrastructure (PKI)).<sup>xxiv</sup>

› **Limit system access (physical or via a network) to authorized individuals for specific purposes through appropriate security controls.**<sup>xxv</sup> Physical security considerations include access to servers, unattended workstations, network wiring, remote access at the operating system or application level, and backup media. In general, access should be based on the principle of least privilege, granting users the minimum permissions necessary to perform their official duties.

› **Ensure only authorized users can create records.**<sup>xxvi</sup> An ERS must include a current list of valid users with associated permissions to read, create, modify, or delete records, as well as contextual information on the authorization and de-authorization of users. Agency policies and procedures must include actions to be taken when a change in a user's status (left, fired, changed position) affects access to the system. Users must not be authorized without proper documentation.

› **An ERS must produce consistent results for the records it creates and must produce identical outcomes for all processes.**<sup>xxvii</sup> Systems should be tested periodically to ensure compliance. For additional information, see ANSI/AIIM Standard TR31-1994 "Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Standards."

<sup>16</sup> The use of interpersonal skills to gain unauthorized access to systems, typically by manipulating individuals with access to the system to relinquish passwords or other authentication tools to an unauthorized individual. The unauthorized individual's manipulations are social engineering.

- 764 › **The ERS should maintain an adequate audit trail of system activity by system or application**  
765 **processes, and by user activity.**<sup>xxviii</sup>  
766

767 For more information, contact the Arizona Auditor General, or see  
768

- 769 › *Practical Tools for Electronic Records Management and Preservation*. Center for Technology in  
770 Government, SUNY. [http://www.ctg.albany.edu/resources/pdfrwp/mfa\\_toolkit.pdf](http://www.ctg.albany.edu/resources/pdfrwp/mfa_toolkit.pdf).

## 771 **Requirements for Access**<sup>xxix</sup>

772 By law, “Public records and other matters in the custody of any officer shall be open to inspection by any  
773 person at all times during office hours” (ARS §39-121). Virtually all documents in the possession or  
774 control of a public officer are considered public records.<sup>17</sup>  
775

776 An agency may refuse access if the record is made confidential by statute,<sup>18</sup> if the record involves the  
777 privacy interests of persons,<sup>19</sup> or disclosure would be detrimental to the best interests of the state.<sup>20</sup> More  
778 than 300 Arizona statutes address confidential records. A complete list may be found in the Arizona  
779 Attorney General’s *Agency Handbook*.<sup>21</sup>  
780

781 If an agency refuses an individual access to records on grounds of personal privacy or the best interests  
782 of the state, the individual may petition a court to review that decision. The court will make a decision  
783 within thirty days, and in most instances the courts have granted the individual access to the records. If  
784 an agency believes that records not specifically closed by law should not be made generally accessible to  
785 the public, it should develop a policy for denying access to or redacting those records. Having a policy in  
786 place ensures that decisions to deny access are well-reasoned and defensible, and avoids any  
787 appearance that the denial is to a specific individual.  
788

- 789 › **The general public must have access to the records.** However, all users must follow  
790 authorization policies and procedures to access the ERS.<sup>xxx</sup>  
791

- 792 › **An ERS must provide adequate search and retrieval capabilities to ensure that e-records can**  
793 **be retrieved for legitimate business purposes throughout their full retention period.**<sup>xxxi</sup> The  
794 ERS should be able to locate likely records when search criteria are incomplete or imprecise. For  
795 example, it should be possible to locate records if a name is misspelled or only part of a name is  
796 name is known.  
797

- 798 › **An ERS should organize the records in a meaningful order to allow for browsing.** Browsing  
799 many individual records that are near matches of the search criteria (similar spellings of a name,  
800 other records from nearby dates, etc.) can enable a user to discover patterns or information that  
801 cannot be formulated in a query.<sup>xxxii</sup>  
802

- 803 › **An ERS must be able to produce authentic copies of records.**<sup>xxxiii</sup> ARS §39-121 requires that  
804 any person may request to examine or be furnished copies, printouts, or photographs of any public  
805 record . . . .” Note, however, that agencies are not required to produce the records in a format  
806 specified by the user. In particular, agencies are not required to produce a subset of data in records  
807 that is formatted for easy manipulation by the user, rather than the official form of the record. For

---

<sup>17</sup> See Carlson, 141 Ariz. at 490, 687 P.2d at 1245. Quoted from Arizona Attorney General, *Agency Handbook*, chapter 6.

<sup>18</sup> Berry v. State, 145 Ariz. 12, 13, 699 P.2d 387, 388 (Ct. App. 1985).

<sup>19</sup> Scottsdale Unified School Dist. No. 48 v. KPNX Broad. Co., 191 Ariz. 297, 955 P.2d 534, 537 (1998).

<sup>20</sup> Board of Regents v. Phoenix Newspapers, Inc., 167 Ariz. 254, 258, 806 P.2d 348, 351 (1991); KPNX-TV, 183 Ariz. at 592, 905 P.2d at 601.

<sup>21</sup> Available online at [http://www.attorney\\_general.state.az.us/Agency\\_Handbook/CHAPTER%206.pdf](http://www.attorney_general.state.az.us/Agency_Handbook/CHAPTER%206.pdf).

example, an agency may be required to produce land records, but is not required to produce a delimited file of names and addresses of property owners in those records.

- › **The agency must develop policies and procedures, some of which would be implemented in the ERS, to protect confidential or private information based on user permissions.**<sup>xxxiv</sup> An ERS must be able to redact confidential or private information. Agencies should be particularly vigilant about releasing such information, which is often present in records in places that are not obvious.
- › **Arizona statute requires that the state be paid for commercial use of records.** The agency should establish policies and procedures to ensure that it is compensated for commercial use of records.

## **Requirements for Maintenance and Preservation**

Manual recordkeeping systems require very little to ensure that they remain useful over time. Records created on paper today can be stored for decades then read, provided they have not been attacked by – for instance – pest, fire, or flood.

Rapid changes in software and hardware make it highly unlikely that an e-record created today could be read after twenty years. Many common office applications (e.g., word processors, spreadsheets) cannot read previous versions that are more than three generations old. Magnetic media is notoriously unstable. The life of data on CD-RW is subject to storage conditions, and can be surprisingly short in less-than-ideal conditions. Even if the data and media survive, there is a good chance that the hardware will not be available to read them; for example, try to find a player for a Beta tape or a 5.25" floppy disk.

To counter these problems agencies must plan to refresh and migrate their e-records. Agencies must also begin to account for these costs in their budgets. These costs are new to agencies, in that it is not necessary to duplicate paper records every five to ten years to ensure that they remain readable. Agencies should consider the costs of migrating systems and the potential risk factors arising from the possible inability to meet those future costs. It may make sense to make copies of high-risk records on a technologically neutral, durable media such as computer output microfilm to ensure a minimum level of access if a system cannot be migrated. Although conversion to a durable media will result in the loss of system functionality, the level of access will support research use of these inactive records.

At some point all software packages will become obsolete, and routine migration will no longer suffice. Successful ERS design must assume and plan for major software or hardware changes by including a mechanism to communicate data from one system to a future system. Because it is impossible to know the nature of a future system, an ERS must be able to export records in a data format that is well documented. Building this export function during the design phase significantly reduces migration costs because the individuals developing the function are intimately familiar with the ERS software and data storage methods.

In particular, digitally signed e-records must incorporate a mechanism to provide adequate validation of the signature over time. Agencies must determine how long it is necessary to authenticate signatures and must establish procedures to verify records that were authenticated by a service that is no longer available.

To ensure that e-records are properly maintained and preserved, the system should address the following requirements.

- › **The content, context, and structure of e-records must be preserved over the life of the record.**<sup>xxxv</sup> E-records created in an ERS must be inviolate, in that they are not damaged, destroyed, or modified; coherent, in that when reconstructed, they represent the logical relations established by the original software environment (and not any updated platform or environment); and auditable, in that all actions taken to a record during the course of its life are documented with a proper audit trail.

- › **Develop retention solutions that are technologically neutral and that balance requirements for use, retention, human intervention, preservation, and security/encryption.**<sup>xxxvi</sup> Solutions should consider the length of time the records must be kept (short-term or long-term, but see below for permanent records), the necessary functionality of the original system, and the need to preserve the context and structure of the records.<sup>xxxvii</sup> Solutions should require minimal human intervention.<sup>xxxviii</sup>
- › **Prefer standard file formats for data.**<sup>xxxix</sup> Document non-standard file formats.
- › **An ERS must be able to export (migrate) records, including their content, context, and structure, to other systems without the loss of information.**<sup>xl</sup> This export function should encapsulate the whole of a record as a single unit or otherwise ensure that the content, context, and structure of the record remains associated. For more information, see Public Records Office Victoria [Australia], *VERS Standard Electronic Record Format* (<http://www.prov.vic.gov.au/vers/standards/pros9907/99-7-3toc.htm>).
- › **Maintain records in encrypted form only as long as security warrants.**<sup>xli</sup> Loss of the encryption key could result in the loss of records. In general, it is best not to rely on encryption to protect the confidentiality or privacy of records when there are no better alternatives to protect the information, such as during transmission over unsecured lines. Encryption should not be used when other measures, such as physical access and authenticity for login, can provide sufficient security.
- › **Agencies should refresh offline data on a routine basis to prevent bit loss or other problems associated with the physical degradation of media.**
- › **Agencies should develop business continuity and disaster recovery policies and procedures.**<sup>xlii</sup> Such policies and procedures should address routine data backup, verification of backups, offsite storage of data, and proper labeling of media.
- › **Agencies should ensure that backup media are overwritten or destroyed in a timely manner so that any obsolete records deleted from the system are not kept significantly longer than the scheduled retention period.** Copies of records on backup media are discoverable, even if the record copy has been deleted from the system. A discovery order could require an agency to search through all extant backup media for relevant records.

## **Requirements for Disposal: Destruction and Archival Storage**

Disposition is the final chapter in the records life cycle, resulting in destruction of the records or their permanent, archival retention. Arizona laws establish a process that determines which records are to be destroyed and how long those records must be kept before destruction, as well as which records must be kept permanently in the State Archives. These laws apply to all records, regardless of format. The ability to demonstrate that records were disposed of legally and routinely is a critical defense against charges of spoliation or tampering with evidence in the case of litigation.

Destruction of records requires that all copies of a record be destroyed. Designing procedures to delete records must address not only the ERS, but copies of data kept for backups, disaster recovery, and the like. System designers should also work with risk managers, archivists, and managers to assess the need to completely erase the data in a manner that makes recovery unfeasible. Media containing records with private or confidential information should be sanitized as part of destruction.

If records are to be kept permanently, then it is essential to develop a strategy to preserve those records. If a decision is made to preserve archival (permanently valuable) records electronically, they must also be transferred to a durable medium (paper or microform). For the near term, this hybrid approach offers the hope that the ERS can be kept live while the durable copies ensure the records are retained in some fashion. The transfer of e-records to durable media should be done in consultation with the State Archives.

To ensure that e-records are properly disposed of, the system design should address the following considerations.

- › **In conjunction with the Records Management Division, schedule all records series in an ERS to establish the appropriate disposition of those records.**
- › **Establish appropriate policies and procedures for system operators to ensure that disposition functions built into an ERS are not compromised.** In particular, aspects of disposition functions that rely on human intervention, such as the destruction or sanitization of media containing records, are properly carried out in accordance with the Arizona Government Information Technology Agency (GITA) Standard for Media Sanitizing/Disposal (P800-S895).
- › **Records destruction should be coordinated with backup and storage procedures so that deleted records are purged on a regular basis.**
- › **Retain records in accessible form for their legal, minimum retention periods as established by Records Management Division.**<sup>xliii</sup>
- › **An ERS must be able to delete or erase records.**<sup>xliv</sup> Design specifications should indicate whether records must be made unrecoverable and, based on risks arising from privacy and confidentiality, the most appropriate method for destroying the data.
- › **An ERS must be able to protect selected records from routine destruction.** In particular, records that may be relevant to pending litigation must not be destroyed, even if those records have passed their retention period.
- › **Records scheduled for permanent retention must be exported to permanent media as defined by Arizona statute, currently paper or microfilm.**<sup>xlv</sup> For preservation of a small set of exceptional records within a large series of records that are not routinely kept permanently, printing to paper may be the most economical and straightforward solution. If a large series is scheduled for permanent retention, computer output microfilm is the best current technology.
- › **Note that the original electronic copies need not be destroyed when a permanent copy is created for the archives.**

## APPENDIX A. ACKNOWLEDGEMENTS

The Arizona ERS Framework is based on the National Electronic Commerce Coordinating Committee's (NECCC) *Electronic Records Management Guidelines for State Governments*. The Arizona Framework also draws on the Delaware Public Archives' *Model Guidelines for Electronic Recordkeeping Systems*. Specific references to those documents are noted in Appendix C.

This document was developed by the Arizona State Library, Archives and Public Records' Arizona 'Electronic Records Taskforce (ALERT). Special thanks to those members actively involved in its development: Richard Pearce-Moses, GladysAnn Wells, Linda Meissner, Brandyn Bolte, William Buchanan, Shanna Chalker, Charles Donofrio, Rich Dymalski, Maureen Haggerty, Jill Harvey, Joseph Hindman, Mark Jensen, Steve Koppen, Elaine LeTarte, Terry Linkous, Gene Martel, Tom Martin, John Messing, Joseph Moore, Patti Nelson, Richard Neshwat, Susan Patrick, William Raiford, Lori Rhyons, Russ Savage, Patti Schofield, Mike Totherow, and Liz Wallendorf.

## **APPENDIX B. ARCHIVAL APPRAISAL CRITERIA**

The Arizona State Archives identifies, collects, preserves, and provides access to records in all formats of Arizona state and local governments and of public officials and other individuals. Archival records remain useful for the Legislature, state agencies, and the general public because those records make government accountable to its citizens; provide evidence about public policies and programs; and protect or verify individuals' rights and entitlements. Archival records provide information about the important people, issues, places, and events that make up the story of Arizona's history.

### **ARCHIVAL VALUE**

The Arizona State Archives is legally mandated to collect and preserve the history of Arizona and its government. The number of archival records is very small, typically two to five percent of the whole of an agency's records.

State Archives and Records Management Division staff work with state agencies and local governments to identify those records with sufficient value to warrant the resources necessary to preserve them in perpetuity and document those appraisal decisions on a records retention schedule. Archivists use their knowledge of Arizona history and their familiarity with other records in the Archives when appraising records. They look for records that add to, complement, or fill gaps in the existing records that document Arizona history.

Archivists use the following criteria in combination to distinguish those records which have lasting value.

- Users
- Creator/Office of Origin
- Evidence of Programs or Functions (Functional Value)
- Content (Informational Value)
- Preservation of Individuals' Rights and Entitlements
- Completeness
- Relationship to Other Records
- Age of the Records
- Format

Agency staff who have questions about which records are archival should flag such records for review by the Archives before they are destroyed, even if the destruction is authorized on a retention schedule.

### **USERS**

The Archives collects records that retain value for its users, the Legislature, state and local agencies, and the general public. The Archives looks for types of records that are supported by existing patterns of use.

### **CREATOR/OFFICE OF ORIGIN**

The Archives collects the records of state and local government in Arizona. Every agency, large and small, creates records which document policies and programs, and those records are valuable to the Archives.

In addition to public records, the Archives also collects the personal papers of public officials and of other individuals or groups if they contain significant information relating to Arizona government, public policies and programs, or the history of Arizona.

To ensure that archival records are authentic and reliable, the content of the records should not have deteriorated through fraudulent change or loss. Changes made by the record creator (or the creator's agent) should be documented so that such changes are readily apparent. Note, however, that there is no requirement that records be accurate; in some instances, it is important to preserve inaccurate records to document that information used to make decisions or to prove fraud.

Records of questionable origin are of questionable archival value. The Archives seeks to collect the original records of the agency which created them or its successor; it generally does not collect copies of an agency's records held by another agency.

Simple association with a notable individual – a mention, a signature – does not, alone, make a record archival.

## **EVIDENCE OF PROGRAMS OR FUNCTIONS (FUNCTIONAL VALUE)**

Records which document the principal responsibilities of the agency or office and that explain programs that help agencies accomplish their missions by documenting the decision making process are likely to be archival. In particular, the Archives seeks to acquire and preserve those records that document the agency's organization, that provide continuity between changes in office, and that demonstrate government accountability.

Administrative records relating to an agency's day-to-day operations are generally not preserved in the Archives. These records include general memoranda, human resources files, facilities files, routine activity reports, and similar records.

Because agencies' policies and programs affect constituents, correspondence and other records documenting public concerns and opinions regarding controversial or divisive policies or programs often warrant archival preservation.

## **CONTENT (INFORMATIONAL VALUE)**

Some records retain their value over time because they contain information about topics that help define the history and character of the state. Records relating to water, agriculture, mining, tourism, urban growth, environmental quality, multiculturalism, and the economy – among other topics – will continue to have archival value. As time passes, new topics will take on archival value.

Records that provide substantial, unique information and background relating to a newsworthy event are often candidates for the Archives.

## **PRESERVATION OF INDIVIDUALS' RIGHTS AND ENTITLEMENTS**

The Archives collects many records that document individuals' enduring rights or benefits under government programs. Examples include, but are not limited to, rights of citizenship, civil status (birth, death, marriage, and divorce), and ownership of real property. The Archives generally does not collect records that detail temporary benefits individuals have received from government programs, such as welfare or public health.

## **COMPLETENESS**

The Archives typically collects an entire record series rather than trying to identify individual files of historical value. (A record series is a group of identical or related records which are normally used and filed as a unit).

In rare circumstances, the Archives may collect sample records from a large series of limited value to document a process or function performed by the agency. Neither the frequency of use nor the size of an individual file necessarily indicate archival value, but use and size may serve as useful flags for more careful appraisal.

## **RELATIONSHIP TO OTHER RECORDS**

The Archives prefers to collect originals, rather than copies, because it is easier to demonstrate the authenticity and reliability of original records.

Records that contain detailed information may be added to the Archives, in addition to summary reports, if other methods of analysis may yield findings significantly different from those in the summary.

A record series is generally not acquired for the Archives if the information contained in those records is routinely repeated in another series that the Archives already collects.

## **FORMAT**

The Archives collects records in all formats, including – but not limited to – papers, photographs, and video and audio recordings. The Archives also collects text, images, and sounds in electronic format.

Format occasionally makes records more valuable because it increases their usefulness. A record series in paper may not be collected in paper format because analysis is impractical. However, that series might be collected if it is in electronic format because use of a computer makes complex analysis practical.

## **AGE OF THE RECORDS**

Archives are not collections of nostalgia and historical curiosities. Age alone does not justify preservation.

The Archives seeks to evaluate all records from the Territorial Period before disposal. These records were often labeled with terms that today would suggest the records are not archival. Closer examination of those records' content may reveal that the description is inaccurate and that the records should be retained permanently.

## APPENDIX C. EQUIVALENCIES IN NECCC AND DELAWARE ERS GUIDELINES

---

NECCC: National Electronic Commerce Coordinating Committee, *Electronic Records Management Guidelines for State Governments*.

D: Delaware Public Archives. *Model Guidelines for Electronic Records*  
(<http://www.state.de.us/sos/dpa/govserv/records%20policies/2model%20guidelines.htm>).

i	NECCC 1.3:91-98, NECCC 2.1.1:124
ii	NECCC 1.2:67-90
iii	NECCC 1.1:14
iv	D2.C.2
v	NECCC 1.3:91-98, NECCC 2.1.1:124
vi	NECCC 2.2:133, 4:423
vii	NECCC 2.1.1:124
viii	NECCC 3.1.1:214, 4.1.1:435, D2
ix	NECCC 4.1:476, 4.1.3:460, 4.1.4:477, 4.2.2:503, 4.1.2:435
x	NECCC 1.1:49, D1
xi	NECCC 2.1:120, 3.1:211, D7, D9
xii	NECCC 4.1.5:488
xiii	NECCC 4.1, D2
xiv	NECCC 4.1.2: 455
xv	NECCC 4.1.3: 460
xvi	NECCC 4.1:476, 4.1.3:460, 4.1.4:477, 4.2.2:503, 4.1.2:435
xvii	NECCC 4.1.5: 488
xviii	NECCC 2.1.1:124
xix	NECCC 2.1:120
xx	NECCC 2.2.4:175
xxi	NECCC 2.3:191
xxii	NECCC 3.2
xxiii	NECCC 2.2.5:183
xxiv	NECCC 2.2:143, 2.3: 166
xxv	NECCC 4.3:520
xxvi	NECCC 2.3:166, NECCC 4.3:520, D8
xxvii	NECCC 4.1:432, 4.2.2:503, D4
xxviii	NECCC 4.1.4: 477
xxix	NECCC 3.3:350, 3.4:358
xxx	NECCC 3.4.4:415
xxxi	NECCC 3.3.1:353
xxxii	NECCC 3.1.2:245
xxxiii	NECCC 3.4:358, NECCC 3.4.4:415
xxxiv	NECCC 3.4.1:362, 3.4.2:366, 4.3:520, D13
xxxv	D9
xxxvi	NECCC 3.2:253, 3.2.4:304
xxxvii	NECCC 3.3: 280ff
xxxviii	NECCC 3.4:300
xxxix	NECCC 3.1.1.2:228, 3.2.1:265, 3.2.7:325
xl	NECCC 3.7:318, D11, D12
xli	NECCC 3.2.2
xlii	NECCC 4.2:495, 4.2.1:498, 4.2.3:514
xliii	NECCC 3.2:253
xliv	D10

